Claims

1. A method of operating a secure network having plurality of network nodes, each node comprising one or more ports, the method comprising the steps of:

locating one or more nodes in a secure location;

Locating one or more nodes in a less secure location;

communicating selected management information from a primary configuration node to all other nodes in the secure network, said communicating having the sub-steps of,

a first port on a first node sending said management information to a second port on a second node via an communication media exclusively shared by said first port and said second port;

allowing no management access to said secure network from nodes located in said less secure locations;

determining a first list of nodes that may send or receive substantive communication in the secure network; and

prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports.

2. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising the recognition, operation and succession of primary configuration node.

3. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints.

4. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions

throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of the primary configuration node, and (ii) node connection controls for designating nodes to participate in the secure network,.

5. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, and (ii) device connection controls that indicate port relationships in said secure network.

6. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, and (ii) management access controls that restrict management services to a defined set of endpoints.

7. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) node connection controls for designating nodes to participate in the secure network, and (ii) device connection controls that indicate port relationships in said secure network.

8. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising, (i) node connection controls for designating nodes to participate in the secure network and (ii) management access controls that restrict management services to a defined set of endpoints.

9. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) device connection controls that indicate port relationships in said secure network, and (ii) management access controls that restrict management services to a defined set of endpoints.

10. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) device connection controls that indicate port relationships in said secure network.

11. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

12. The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node (ii) device connection controls that indicate port relationships in said secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

13. The invention of claim 1 wherein the step of allowing no management access to said secure network from nodes located in said less secure locations comprises the sub-step of distributing a MAC list to every node in said secure network, said MAC list comprising an indication of network endpoints from which management access is acceptable.

14. The invention of claim 13 wherein said network endpoints comprise IP addresses.

15. The invention of claim 14 wherein said IP addresses are associated with access from SNMP or Telnet or HTTP or API.

16. The invention of claim 13 wherein said network endpoints comprise uniquely identified ports.

17. The invention of claim 13 wherein said network endpoints comprise uniquely identified nodes resident in said secure network.

18. The invention of claim 1 wherein the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network.

19. The invention of claim 1 wherein the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network.

20. The invention of claim 19 wherein said ports are identified by a unique number.

21. The invention of claim 20 wherein said unique number is a world-wide-name.

22. The invention of claim 1 wherein said directly connected ports are said first port and said second port and wherein the step of authenticating a link between said directly connected ports comprises the sub-steps of:

sending a first fact from said first port to said second port;

at said second node, creating a second-type derivative of said first fact,

sending said second-type derivative of said first fact from said second port to said first port;

at said first node, storing said second-type derivative of said first fact in a first memory;

sending a second fact from said second port to said first port;

at said first node, creating a first-type derivative of said second fact;

sending said first-type derivative of said second fact from said first port to said second port;

at said second node, storing said first-type derivative of said second fact in a second memory;

sending defined information concerning said first node from said first port to said second port;

sending a third-type derivative of said defined information concerning said first node from said first port to said second port;

at said second node, comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node;

at said second node, comparing said first type derivative of said second fact with said second fact;

sending defined information concerning said second node from said second port to said first port;

sending a third-type derivative of said defined information concerning said second node from said second port to said first port;

at said first node, comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node; and

at said first node, comparing said second type derivative of said first fact with said first fact.

23. The method of claim 22 wherein the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of:

reversing the derivation of the third-type derivative of said defined information concerning said second node; and

comparing the result of said reversal with said defined information concerning said second node.

24. The method of claim 22 wherein the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of:

making a third-type derivative of said defined information concerning said second node; and

comparing the made third-type derivative with the received third-type derivative.

25. The method of claim 22 wherein the step, at said second node, of creating a second-type derivative of said first fact comprises the sub-steps of:

encoding said first fact to yield an encoded first fact; and

encrypting said encoded first fact.

26. The method of claim 25 wherein said encoding is performed by applying a hash function.

27. The method of claim 25 wherein said encrypting is performed using a private key unique to said second node.

28. The method of claim 22 wherein said defined information concerning said first node comprises encryption key information.

29. The method of claim 28 wherein said encryption key information comprises a public key uniquely associated with said first node.

30. The method of claim 22 wherein said third-type derivative is associated with both said second node and said first node.

31. The method of claim 30 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first node and said second node.

32. The method of claim 30 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority being the manufacturer of either said first node or said second node.

33. The method of claim 22 wherein the step, at said second node, of comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node, comprises the sub-steps of:

reversing said third-type derivative of said defined information concerning said first node yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information concerning said first node.

34. The method of claim 33 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority associated with said first node and said second node.

35. A specific networking node operating in a secure network, said secure network having a plurality of network nodes, each node comprising one or more ports, said specific networking node comprising:

a first port on said specific networking node for receiving selected management information from a primary configuration node, said first port directly communicating with a second port on a second node via an communication media exclusively shared by said first port and said second port;

a memory for storing (i) management access information, and (ii) device connection information specifying nodes or ports that may send or receive substantive communication in the secure network; and

a processor for causing the authentication of the link between said first port and said second port prior to substantive communication between said first and second ports.

36. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising the recognition, operation and succession of primary configuration node.

37. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints.

38. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions

throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of the primary configuration node, and (ii) node connection controls for designating nodes to participate in the secure network,.

39. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, and (ii) device connection controls that indicate port relationships in said secure network.

40. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, and (ii) management access controls that restrict management services to a defined set of endpoints.

41. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) node connection controls for designating nodes to participate in the secure network, and (ii) device connection controls that indicate port relationships in said secure network.

42. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising, (i) node connection controls for designating nodes to participate in the secure network and (ii) management access controls that restrict management services to a defined set of endpoints.

43. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) device connection controls that indicate port relationships in said secure network, and (ii) management access controls that restrict management services to a defined set of endpoints.

44. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) device connection controls that indicate port relationships in said secure network.

45. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

46. The invention of claim 35 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node (ii) device connection controls that indicate port relationships in said secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

47. The invention of claim 35 said management access information comprises a MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable.

48. The invention of claim 47 wherein said network endpoints comprise IP addresses.

49. The invention of claim 48 wherein said IP addresses are associated with access from SNMP or Telnet or HTTP or API.

50. The invention of claim 47 wherein said network endpoints comprise uniquely identified ports.

51. The invention of claim 47 wherein said network endpoints comprise uniquely identified nodes resident in said secure network.

52. The invention of claim 35 wherein said device connection information comprises a DCC list, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network.

53. The invention of claim 35 wherein said device connection information comprises a DCC list, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network.

54. The invention of claim 53 wherein said one or more other ports are identified by a unique number.

55. The invention of claim 54 wherein said unique number is a world-wide-name.

56. The invention of claim 35 wherein said specific networking node further comprises:

a second memory for storing a first secret fact;

a third port for sending said secret fact to a third node;

a fourth port for receiving,

a second-type derivative of said first secret fact from said third node,

pre-defined information about said third node, and

a third-type derivative of said pre-defined information about said third node; and

said processor also for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said third node and said third-type derivative of said pre-defined information about said third node.

57. The invention of claim 56 wherein said third port and said fourth port are the same port.

58. The invention of claim 56 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes reversing the derivative nature of said second-type derivative of said first secret fact.

59. The invention of claim wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes creating a second-type derivative of said first secret fact.

60. The invention of claim 56 wherein said second-type derivative is associated with said third node.

61. The invention of claim 56 wherein said third-type derivative is associated with said specific networking node and said third node.

62. In a network having a plurality of devices, wherein at least one of said devices is a switch or router, and all devices are communicatively coupled together, a method of securing said network, comprising the steps of:

mutually authenticating all links in the network, where a link is a bi-directional communication apparatus between two devices;

limiting access to a first set of one or more management functions by allowing control of said first set of management functions only through one or more pre-selected devices; and

limiting access to a second set of management functions to access only through one or more pre-determined logical channels of said devices as specified by a network operator.

63. The method of claim 62, further comprising the step limiting communication to that occurring between pre-defined pairs of said devices.

64. The method of claim 62, further comprising the step of limiting devices in the logical network to those on a pre-defined list of allowed devices.

65. The method of claim 62 where there is only one pre-selected device.

66. The method of claim 62 wherein said pre-selected devices are all located in controlled-access environments.

67. The method of claim 62 where the first set of management functions is mutually exclusive from the second set of management functions.

68. The method of claim 62 where the first set of management functions is identical to the second set of management functions.

69. The method of claim 62 further comprising the step of providing a distributed time service

70. The invention of claim 69 wherein said distributed time service is provided by the sub-steps of

entering the time using an input mechanism on a first timekeeping device;

sending the time from said first timekeeping device to a primary timekeeping entity;

broadcasting a time update from said primary timekeeping entity to all other timekeeping entities, said broadcast repeating every T1 seconds and carrying an indication of the current time;

receiving said time update at a second timekeeping entity and starting a counting device upon said receipt;

checking the status of the counting device every T2 seconds and determining the elapsed time since said second timekeeping device received said time update; and

comparing said elapsed time to a predetermined threshold value T3; if said elapsed time is greater than T3, making an indication that said second timekeeping device's time is unreliable.

71. The method of claim 62 wherein the network comprises a Fibre Channel fabric.

72. A method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together, said method comprising the steps of:

only allowing communication between pre-defined pairs of said devices as specified by a network operator; and

only allowing substantive communication between devices that are on a pre-defined list of allowed devices, said pre-defined list stored on a memory in each of said plurality of devices; and

only allowing substantive communication between directly connected ports that have been mutually authenticated.

73. A network comprising:

a plurality of devices including one or more switching and routing devices, any two of said devices able to inter-communicate only by direct links between each

other, all devices able to inter-communicate by forwarding communications through each other;

all of said devices capable of mutually authenticating directly connected links;

one or more pre-designated devices for facilitating management-level control of the network; and

all of said devices carrying a list of all devices allowed on the network.

74. The invention of claim 73 where the network is a Fibre Channel fabric and all the devices are routing and switching devices.

75. The invention of claim 73 wherein said pre-designated devices are each in a room having a locking mechanism to control human ingress and egress.

76. A routing device for receiving and directing information in a network, comprising:

a public and private key pair;

one or more ports for coupling to other routing devices and for authenticating said other routing devices and for communicating using said public and private key pair;

a memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network; and

a least one logical management access channel that may be disabled through network management control.

77. The invention of claim 76 where a certificate authority for the public and private key pair is not the entity controlling management access to said routing device

78. The invention of claim 76 further comprising a memory for storing distributed time service information.

79. A network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity and (ii) switch connection controls for designating devices to participate in the secure network, said network configuration entity comprising;

a memory for storing

an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity;

an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network..

a first secret fact;

a first port for sending said secret fact to a second switch;

a second port for receiving,

a second-type derivative of said first secret fact from said second switch,

pre-defined information about said second switch, and

a third-type derivative of said pre-defined information about said second switch; and

a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch.

80. The invention of claim 79 wherein said first port and said second port are the same port.

81. The invention of claim 79 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes reversing the derivative nature of said second-type derivative of said first secret fact.

82. The invention of claim 79 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes creating a second-type derivative of said first secret fact.

83. The invention of claim 79 wherein said second-type derivative is associated with said second switch.

84. The invention of claim 79 wherein said third-type derivative is associated with said network configuration entity and said second switch.

85. The invention of claim 79 wherein said pre-defined information about said second switch comprises encryption key information.

86. The invention of claim 79 wherein said first secret fact is a random number.

87. The invention of claim 79 wherein said first secret fact is a nonce.

88. A method of maintaining distributed time in a network having a plurality of timekeeping devices including a primary timekeeping entity, said primary timekeeping entity also being a network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) switch connection controls for designating devices to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints, said method comprising the steps of:

entering the time using an input mechanism on a first timekeeping device;

sending the time from said first timekeeping device to said primary timekeeping entity;

broadcasting a time update from said primary timekeeping entity to all other timekeeping entities, said broadcast repeating every T1 seconds and carrying an indication of the current time;

receiving said time update at a second timekeeping entity and starting a counting device upon said receipt;

checking the status of the counting device every T2 seconds and determining the elapsed time since said second timekeeping device received said time update; and

comparing said elapsed time to a predetermined threshold value T3; if said elapsed time is greater than T3, making an indication that said second timekeeping device's time is unreliable.

89. A method of maintaining distributed time in a network having a plurality of timekeeping devices including a primary timekeeping entity, said primary timekeeping entity also being a network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure

network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) switch connection controls for designating devices to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints, said method comprising the steps of:

checking all timekeeping devices to determine if each is capable of participating in a secure time distribution system;

at the primary timekeeping entity, ascertaining the time and constructing a time update item;

creating a first-type derivative of said time update item;

creating a time update message comprising said time update item and said first-type derivative of said time update item;

sending the time update message to all timekeeping devices; and

at a first timekeeping device receiving said time update message, processing said time update message, wherein processing said time update message includes the sub-steps of, (i) noting a time of arrival and storing said time of arrival in a first memory; (ii) starting a counter to measure the age of the received time update at a time interval Tmeasure; (iii) storing in a second memory, the time from said time update message; (iv) creating a second-type derivative of said update item; and (v) comparing said created second-type derivative of said update item with the received first-type derivative of said update item.